

Title: LTE-based public safety broadband network design and test process proposal	
From: Aeroflex	To: FCC
Document number: UDA-343	Version: A10
Date: 2011 02 23	

Table of Contents

1	Background.....	2
2	Executive summary	2
3	LTE-based public safety broadband network.....	3
4	Current Validation Process for Commercial Networks	4
5	Public Safety Infrastructure Test Challenges.....	8
6	Ideal Infrastructure Test Process for Public Safety	10
7	Conclusions	15
	REFERENCES:.....	16
	APPENDIX A: LTE Overview	17
	Appendix B: Technology Life Cycle Test Equipment	21
	Appendix C: KPI Complete List	29
	Appendix D KPIs Table	32

1 Background

The Federal Communications Commission (FCC) and Congress have created the public safety 700MHz broadband spectrum allocations over several years and rulings. The federal government has further mandated that there be a nationally interoperable public safety network based on the LTE standard as defined by 3GPP, the telecommunications industry standards body. The National Telecommunications and Information Association (NTIA), via the BTOP program, has started granting federal funds for public safety network roll outs.

The Public Safety Communications Research (PSCR) program acts as an objective technical advisor and laboratory for critical public safety communication standards and technologies. As part of their role, PSCR will be deploying and operating a demonstration and evaluation LTE network for public safety broadband. This network will serve the dual purpose of demonstrating the technological capabilities and allow public safety entities to evaluate infrastructure vendor's equipment against a live public safety network.

2 Executive summary

Per FCC order, the PSCR is evaluating infrastructure equipment for waiver recipients in their demonstration network. Additionally, nearly \$400 million has already been granted across 7 public safety entities for the initial network roll out and more monies will be granted via federal stimulus projects in the coming months. All mobile devices which connect to the public safety network will also be required to follow the same rigorous process as commercial devices. Mobile device vendors will need to submit their devices through the PTCRB process at an accredited PTCRB conformance laboratory both for radio frequency (RF) and protocol requirements.

"On the infrastructure side, there are very few places where you can do interoperability testing [today]," admits Emil Olbrich of the PSCR. [2] In a typical commercial network, the network operator works with their infrastructure vendors to validate that their equipment conforms to both the industry requirements and the operator proprietary requirements. Since there is no single designated network operator in the public safety network, there is also no designated entity that will assure infrastructure equipment meets acceptable performance requirements.

This paper proposes a possible solution to this complex and critical challenge. The paper will describe the current commercial infrastructure testing process as well as detail how to leverage existing resources and organizations to create an acceptance process for public safety infrastructure.

This paper will not cover inter-vendor interoperability testing beyond how different network elements interoperate. The paper also does not make judgement on the merits of a network of networks versus a single network approach for implementation or management of the final network. The assumption throughout the paper is that there will be a network of networks each with a unique packet core and local governance. Finally, the paper does not aim to overtly address the issue of enforcement of compliance to the process as this is heavily influenced by both federal and regional legislation and outside the scope of a technical discussion.

The proposal entails only one major change to the current PSCR demonstration network process: there should be some pre-defined entrance criteria to the network. The public safety industry should have the same tools and safeguards as commercial operators. As proposed, the entrance criteria will be in the form of easily measurable key performance indicators (KPIs) created with assistance from industry and all testing will be performed by approved vendor labs and/or approved independent labs. Only once the vendor has passed the entrance criteria will they be given access to the PSCR network and only once they have gone through the PSCR network will they be approved to sell their equipment to public safety entities. Public safety entities who install network equipment without first going through the process could be subject to punitive action including any combination of withdrawal of funding, abrogation of spectrum or some type of fine. This will, of course, be subject to both federal and local legislation.

Implementing the straight-forward process will give public safety entities a level of confidence in the equipment they purchase and deploy, as well as help ensure the success of the public safety LTE network.

3 LTE-based public safety broadband network

3.1 LTE Public Safety Overview

To help move forward broadband technology for public safety communications, PSCR is building a national public safety broadband demonstration network and providing technical advocacy for the public safety community through requirements gathering and standards development.

Given its technological advancements and global scale, LTE (long term evolution) technology has been selected for the public safety broadband network deployment over Band XIV (788-798 MHz uplink and 758-768 MHz downlink), which aims to provide a wide variety of rich media applications enabling the public safety agencies to have real-time access to mission critical information from anywhere at anytime enhancing the situational awareness. This new generation of public safety broadband network will transform the public safety services making them more reliable, more effective and more efficient during routine operations and during catastrophic events.

For more information on LTE specifics please see Appendix A.

3.2 Status of Commercial Rollout

Currently there are four major commercial operators in the United States and two new entrants actively rolling out or testing LTE networks. Metro PCS has already rolled out a LTE network in five major markets with more cities being added regularly. Verizon plans to have a functioning LTE network in 38 major US cities by the end of 2010. AT&T plans to turn on LTE networks in large cities early in 2011. Lightsquared, a new company, is rolling out a nationwide LTE wholesale network for use in non-traditional markets such as oil drilling communication, smart grids, etc. Both Sprint and Clearwire are actively testing LTE. Globally, LTE is the fastest growing wireless technology.

3.3 Status of Public Safety rollout

There are approximately 50,000 public safety entities using a combination of different and typically non-interoperable technologies for emergency communication and first responders. The US federal government, via the FCC's broadband plan, has mandated the deployment of a nationwide, interoperable LTE telecommunication network in Band XIV to supplement the existing network.

The national network will take years to roll out across all 50,000 public safety entities and it will take even longer for all existing technologies to be phased out. In the mean time, managing the rollout to assure that all technologies are interoperable and co-exist without interference will be critical.

Emil Olbrich goes on to state "For public safety we're looking at a network that has multiple vendors in it. And when you have multiple vendors there are multiple interfaces that are implemented in different way. Ensuring that those are tested and ensuring that they work together for mission critical data and voice is key." [2] The US Congress set aside \$4.7 billion toward the FCC broadband plan, much of which was to be spent for public safety wireless network rollout. \$400 million has already been allocated toward initial small network roll outs across 7 different programs. Many more programs are still seeking funding both via the federal government and through other mechanisms. Additionally the federal government has requested funding for another \$10.7 Billion for a nationwide LTE public safety roll out. The PSCR evaluation network should be fully functional early in 2011 with the first public safety entities turning on their networks shortly thereafter. The rollout will likely continue over the course of the next decade.

4 Current Validation Process for Commercial Networks

Network infrastructure vendors follow a rigorous process prior to deploying their equipment in the field. In addition to extensive development and design testing, they must conform to their customer's requirements. Network operators develop and enforce test specifications based on a combination of 3GPP test requirements and proprietary test scenarios. Often infrastructure equipment vendors must follow unique test processes for multiple network operators.

4.1 Overview

All infrastructure vendors must go through the same high-level process prior to deploying their equipment in a live network.

- They must perform development/design testing using internal specifications based on the published standards.
- They must perform pre-acceptance testing to ensure that their equipment meets their customer's requirements.
- Once the equipment passes internal testing it is delivered to the customer (i.e. network operator) or a customer's designated laboratory for customer acceptance testing based on the customer's proprietary test specification.
 - The customer acceptance testing typically includes RF conformance validation against the 3GPP specification
 - Acceptance test also includes protocol conformance based on a mix of 3GPP and customer internal requirements.
- Finally, the equipment must undergo "real-world" testing in a live network including verification of interoperability with other network equipment and mobile devices as well as drive testing.

This thorough process ensures that all issues are caught as early as possible, decreases time to market and minimizes issues found during and after deployment.

4.2 Development/Design Testing

The infrastructure equipment vendor will validate their equipment against internal design specifications. The design will have been based on the 3GPP standard so a large part of the internal testing will have its foundation in the 3GPP requirements specifications. Additionally much of the test environment will mimic the test configurations from later process steps to ensure that defects are caught as early as possible.

4.3 Pre-acceptance testing

Infrastructure vendors develop extensive internal test plans consisting of all the required test scenarios from all of their customers. They perform these tests prior to submitting their equipment for acceptance by each network operator. Since the issues are easier and cheaper to resolve before customer delivery, pre-acceptance testing is very important to infrastructure vendors.

Performance, stress and real-world scenarios are often emulated and tested during the pre-acceptance stage of testing. Examples of the tests that are run in this stage are listed under the Acceptance Testing section below.

4.4 Acceptance testing

Network operators require infrastructure equipment to undergo a combination of RF, protocol and performance testing.

4.4.1 RF Conformance Testing

All infrastructure equipment manufacturers are required to pass 3GPP 36.141 or 36.142 LTE RF conformance tests. This testing is traditionally performed in a laboratory environment using RF test equipment. Network operators often define test configurations and environments. The 36.141 and 36.142 tests focus on RF parametric requirements of the infrastructure such as output power, error vector magnitude, adjacent channel leakage, CQI measurements, etc.

4.4.2 Protocol Test Scenarios

In addition to RF testing, the infrastructure vendors must also validate that their equipment conforms to LTE protocol requirements. This testing is traditionally performed in a laboratory environment with mobile equipment emulators. Network operators often define test configurations and environments including acceptable test equipment.

The following are a few examples of tests that infrastructure vendors run for this type of testing:

- **Environment** – These tests are all run in a laboratory environment using emulated mobile devices or user equipment (UE). In some cases a single UE is emulated, in other multiple emulated UE's are required. Most of the testing is run in an automated fashion, sometimes remotely over long periods of time.

- **Call setup testing** – The call admission should be one of the first protocol procedures to be tested. The UE emulator periodically sends a lot of RACH (random access channel) requests to the eNB on the uplink with some randomized or specific RACH procedure parameter values (such as the RACH preamble power ramps-up step size). This tests the LTE RACH detector in the eNB and the eNB's ability to handle and control the RACH loading. The test controller of the eNB can also instruct the eNB to send paging signal to the emulated UE's to switch them from idle mode to connected mode. The commercial eNB is normally tested with hundreds of call setup and release procedures periodically over a period of few seconds.
- **Authentication testing** – In LTE, both the eNB and the UE can initiate the authentication procedure. The eNB should be tested with a large number of UE's requesting authentication and the eNB can initiate the authentication procedure with the emulated UE's. The emulated UE's can be configured to give false information to test the eNB's response to malicious attacks.
- **Sub-layer testing** – It is important for the commercial equipment vendors to test the different sub-layers of the protocol layer independently. The test solution must enable incremental testing at Layer 1, Layer 2 or higher layer levels. The performance of each sub-layer is evaluated using complex tests scenarios.
- **Automated boundary testing** – The test solution must give a large amount of detailed debugging information and enable test case creation over a broad parameter space including the special corner cases. The test solution should make it possible to alter parameters in real time to extend test coverage across a wide range of different configurations used in a live system. This enables early detection of software bugs that may not otherwise be found until much later in the development cycle when diagnosing and rectifying errors is typically much more expensive.
- **Scheduler testing** - The scheduler design is a major performance distinguisher for the eNB's among different vendors. The common approach in commercial LTE development is to use test equipment which emulates multiple UE's, allowing the developer to control precisely the mobility profile for each UE in the system. This way, infrastructure vendors can create specific scenarios that cause problems for the eNB scheduler. Then they can adjust the scheduler parameter or algorithm and rerun the test until it gives good results.
- **Handover testing** – Test equipment that is capable of emulating a single UE over the air can be used to test eNB's in both inter frequency and intra frequency handover scenarios during field trials. Both the handover measurement procedure and the handover protocol procedure can be evaluated by the over the air field trials.

In the lab, the multi-UE test equipment can be used to emulate a large number of UE's performing handover simultaneously to stress the eNB and the network's ability to handle the scenarios like many passengers in a high speed train moving across the cell boundary.

- **Interference management testing** – The interference coordination procedure is another important aspect of the LTE system, improving the cell edge throughput and coverage. To test interference coordination, the tester will need a multi-UE emulation platform and a test controller that can send information of the emulated interference scenario to the eNB under test. The scheduling and resource allocation algorithms and the downlink power control procedure of the eNB can then be evaluated in a very controlled and precise manner in very complicated interference scenario that changes rapidly in real-time.
- **Capacity and load testing** – All the network elements and the integrated network itself must be stress tested under very heavy traffic loads from a large number of users close to or beyond the system limits. A network capacity test system is typically used to emulate very realistic and large scale network scenarios including the eNB and the core network elements. This test solution evaluates the capacity of the overall network by generating a large load from thousands of UE's with different mobility, traffic and application models helping to identify the bottleneck of the integrated network.
- **Stability testing** – Before or after the network is deployed, it is inevitable that the software (SW) and firmware will need to be updated for enhancements or bug fixes. It is important to evaluate the performance and stability of the SW before it is distributed to the real and operating network. Therefore, the SW changes must be tested and evaluated extensively in a lab test environment that emulates the real and operational networks. The commercial LTE vendors normally test their new SW or system releases using a set of very comprehensive, automated tests non-stop for at least 2 weeks for every major SW or firmware upgrade.

For more information on the complexities of testing LTE infrastructure and more detailed description of LTE infrastructure test equipment please see Appendix B.

4.4.3 Beyond the laboratory

4.4.3.1 Interoperability Testing and Plug-fests

In addition to the laboratory testing, infrastructure vendors are required to perform extensive testing in real world environments. They must assure that their infrastructure equipment works with a variety of mobile terminals, other vendor's infrastructure equipment, and different core network elements in live network configurations. Network operators will often sponsor plug-fests and network trials to bring all the appropriate stake holders together. The laboratory testing is typically a pre-requisite for invitation to "real world" test activities, but the testing in these network sponsored events is much more critical to success in the long term. This is where the network operator learns how the equipment will work once deployed and finds all the high risk areas and points of failure.

According to Kenneth Budka of Alcatel Lucent, "Inter-vendor testing is the most important thing for making sure that device from any vendor work. This happens today among competitors. It doesn't happen naturally. It happens as a result of contracts and requirements for equipment. Our customers come to us and say they're building a network and we need to test it. It is that testing that insures interoperability across networks and vendors. It is a must. You do not get your check if you do not go through the testing."[1]

4.4.3.2 Field and Drive Testing

Finally, after the plug-fests and network trials are completed, infrastructure vendors must subject their infrastructure equipment to field testing with either real or emulated mobile devices in mobility scenarios. Typically the equipment is setup exactly as it will be once it's deployed in a small subset of the full network. Then testers will drive around a pre-determined path and verify handover scenarios, interoperability scenarios, performance limitations, etc.

Mr. Budka further mentions, "One of the most important things for building an interoperable public safety or commercial network is actually rolling that network out into a field setting and testing the things you cannot test in a laboratory environment. This is something called First Office Application and something that is an absolute necessity for public safety as well." [1]

4.4.4 Final Acceptance

Only once the infrastructure has passed all of these test areas will the network operator deploy the equipment across their network. In order to limit exposure to risk and keep costs within reasonable bounds, network operators often cap the number of infrastructure vendors to 2 or 3.

5 Public Safety Infrastructure Test Challenges

The information in this section references specifications currently being developed by the PSCR and is based on the latest information published by the PSCR. All PSCR updates and corrections will be incorporated in this paper prior broader dissemination. As the PSCR updates their documentation, this whitepaper will also be updated.

5.1 Public Safety Requirements

The nature of public safety communication makes it different than commercial telecommunication at a basic level. An emergency situation may require clearing the network to save capacity only for responders to the emergency. Some network interactions will take precedence over others and some network users will always need to pre-empt others. The PSCR is developing a complete list of requirements specific to public safety network infrastructure.

Although most of these requirements fit within the current standard 3GPP definition of LTE, very few network infrastructure vendors have implemented the parts of the standard outside of commercial requirements. "There are pieces of the network that will be unique to public safety. The network elements themselves are going to have some special features for quality of service, pre-emption and other things that have to be used in a way that is standard across all vendors and networks so that this works as need for public safety," says Emil Olbrich. [1]

Here are a few examples of requirements that will likely necessitate significant development and testing for infrastructure vendors beyond commercial specifications:

- Cell Barring
- Cell Reservation
- Special Access Classes
- User Pre-emption
- Application Pre-emption
- Etc.

5.2 PSCR Unique Test Scenarios

In addition to the unique network infrastructure requirements of the public safety network, public safety use cases of the network differ significantly from commercial use cases. Natural disasters, terrorist attacks, plane crashes, etc. require a network and user interaction very different from every day life. The emergency area may be located at cell edge and bring an abnormal number of users to the area, thus putting significant strain on the network. This network strain cannot bring service down in the emergency. So, the network must be dynamic and robust enough to handle the situation.

Additionally, even with all the various wireless communication improvements that 700 MHz LTE brings, there will always be inherent challenges with getting complete in-building penetration and ubiquitous coverage. A combination of femtocells, network repeaters and mobile picocells will be required to extend the network inside of building with high interference or weak coverage and to add coverage to cell edge in emergency situations. These additional network infrastructure nodes will need to be taken into account for future public safety test scenarios.

The PSCR is developing a comprehensive list of public safety specific scenarios. Here are a few examples:

- Networks that provide voice service as an application should provide voice interoperability interfaces to existing agency LMR systems in the area served by the broadband network.
- Public Safety users dual technology home or visited networks should be able to call or hail an authoritative dispatch agency or control point using the broadband network subscriber device with microphone and speaker for two-way audio and talk or be connected to other serving agency voice communications resources.
- Regional networks should include the capability to collect and convey subscriber unit location data in real time. Location data should be accessible to appropriate applications, as may be authorized by management level policy.
- Subscriber units of future public safety networks should meet the same minimum location data information requirements (format and accuracy) as is currently applicable on current commercial services networks in order to retain a broad level of compatibility with incumbent systems
- Regional networks should provide one-to-many communications capabilities to outside network users responding in mutual aid to that regional network. These communications capabilities should extend from voice, as commonly used in traditional land mobile radio systems, to text messaging, to video, and other forms of data communications.

6 Ideal Infrastructure Test Process for Public Safety

In order to assure that infrastructure equipment in public safety conforms to the 3GPP specifications and to national public safety network requirements, it is vital that there be a nationally accepted conformance/acceptance process. Unlike in the commercial operators, there is no single, national entity responsible for nationwide interoperability or conformance to minimum requirements. As Emil Olbrich of the PSCR points out, "Each [requirement] is implemented differently by every single vendor and just because a standard is developed that doesn't mean that everything in the standard is put into a box. For example, 3GPP Release 8, December 2009 release I would venture to guess that not one vendor has deployed all the features that are available in release 8. They just don't do that. They do that based on the needs of the vendors, carriers, customers and what they request. So, being able to test against each of those implementations against each other is key. How they get implemented, 3GPP doesn't really define that." [2]

However, with minimal process changes this paper contends that key practices from the commercial operators can be replicated for public safety networks.

The PSCR is developing a demonstration and evaluation network that has started evaluating public safety infrastructure equipment. Additionally there is already an industry standard conformance specification for LTE infrastructure RF requirements. Ideally, the PSCR will take the extra step of adding laboratory testing as gating criteria to entering the evaluation network. In a manner to be decided, vendors would need to pass RF and protocol tests prior to acceptance by the PSCR. Using this new process the public safety governing organizations can be assured that all public safety infrastructure equipment meets a level of quality that is sufficient for use by public safety entities nationwide.

Edmond J. Thomas from Wiltshire and Grannis makes the point that, "If you choose different vendors for state networks, obviously they have to be certified as interworking. So that brings with it the requirement that the NTIA and the FCC put together a test spec to show that the networks basically meet the standard." [3]

It is particularly important that public safety infrastructure conforms to a common standard so that emergencies that occur across multiple public safety entities do not have interoperability problems.

6.1 Development/Design Testing

The development/design test process for PSCR should be identical to the commercial test process except for any tests explicitly added to the 3GPP specification for PSCR.

6.2 Acceptance testing

Since there is no single network operator in public safety, the PSCR will ideally communicate which tests will be required for entry into the PSCR evaluation network. PSCR has already started developing an evaluation network test plan. Minimally, the PSCR will require that all of this testing is performed successfully in the laboratory prior to allowing the equipment into their evaluation network.

With industry input, they may also expand these minimum criteria to include additional laboratory testing. Jeff Anderson from Motorola solutions believes that for public safety, “something very unique here going forward with 3G and 4G technologies... the performance realized in the network is heavily dependant on scheduling algorithms in the base station which are not specified. They are vendor implemented and they vary over release and over timeframe.”[3]

6.2.1 RF Conformance Testing

The PSCR will require that some subset of the 3GPP 36.141 or 36.142 RF conformance tests are passed prior to accepting equipment to their evaluation network.

Following are the 3GPP RF Conformance tests currently being considered as part of the PSCR evaluation test plan:

- 6.2. Base station output power
- 6.3.2. Total power dynamic range
- 7.2. Reference sensitivity level
- 7.3. Dynamic range
- 7.4. In-channel selectivity
- 7.5. Adjacent Channel Selectivity (ACS) and narrow-band blocking
- 7.6.5.1. Blocking (General requirements)
- 8.2.1. Performance requirements of PUSCH in multipath fading propagation conditions
- 8.3.2. CQI missed detection for PUCCH format 2 (crucial for MIMO operation)

6.2.2 Key Performance Indicators

When attempting to replicate the minimum standards of commercial network operators, it is much more important that a public safety network equipment meet specific industry needs than a series of esoteric technical requirements. To this end, this paper proposes a set of key performance indicators (KPIs) to be used as a minimal standard for entry into the PSCR evaluation network. The KPIs must be discrete, measurable and generic so that they are entirely objective in demonstrating the ability of the network equipment to fulfill the specific requirements of the public safety network.

Initially the list of KPIs should be kept relatively small to focus on the core features and to encourage adoption of the process. As the network matures, the KPI list should grow and include new measures of quality based on experience in the field. It will be necessary for some organization to maintain the KPI list and update it based on updated LTE specifications, market conditions and input from both the public safety community and the vendor marketplace. This organization should be federal in scope and technically capable enough to take into account all relevant factors. An example of one such organization is the PSCR.

With assistance from the public safety community, Aeroflex has compiled the following list of core KPIs to use as the initial entrance criteria into the PSCR evaluation network:

1. RACH and Paging
 - a. Radio bearer setup success rate, at varying (increasing) numbers of attached UEs with steady user-plane eNB throughput (both uplink and downlink)

- b. Dropped default bearer rate, at varying (increasing) numbers of attached
 - c. UEs with steady user-plane eNB throughput (both uplink and downlink) and varying bearer setup rates and paging rates
 - d. Paging success rate at varying levels of paging requests per second
 - e. Paging response time
 - f. Attach request setup time with simulated UEs and simulated EPC (with increasing number of attached UEs per cell)
2. User Experience and Stress
- a. Downlink end-to-end EPS delay
 - b. Uplink end-to-end EPS delay
 - c. Downlink UDP file transfer time
 - d. Uplink UDP file transfer time
 - e. Time to active calls upon base station failure.
 - f. In addition to attach request setup time you might consider call setup time.
 - g. Average setup time over a varying (increasing) number call setup and release procedures.
 - h. - Maximum number of simultaneous authentication requests the eNB can handle without failure
 - i. Inter-cell and Intra-cell Handover both by a single user and multiple users simultaneously.
 - i. Measured by time to handover
 - ii. Measured by maximum number of users that can simultaneously handover
 - j. Maximum throughput at full load
 - i. Will measure the number of users the eNB can handle with active data connections at different throughput loads
 - ii. i.e. 50 users with 250k connections, 12 users with 1MB connections, etc.
 - k. Near cell with no loading vs Edge of cell with high loading
- I. Application Performance
- i. Ping
 - ii. FTP Downlink
 - iii. FTP Uplink
 - iv. VPN Email send and receive
 - v. Web Browsing
 - vi. Video Downlink and Uplink streaming

Some of these KPI's will only be properly verified once the network has been deployed in the field. Some subset of the KPI's listed above will need to be measured in each of the main environmental conditions represented in the public safety entity's region. Those environmental conditions include:

1. Population density
 - a. Urban dense (i.e. morning rush hour)
 - b. Urban sparse (i.e. late night)
 - c. Suburban
 - d. Rural
 - e. Etc.
2. Topography
 - a. Mountainous
 - b. Forested
 - c. Desert/High plains
 - d. Urban with dense high rise buildings
 - e. Urban with sparser low buildings.
 - f. Etc.

Additional potential KPI's and further description of the KPIs listed can be found in Appendix C and D.

6.2.3 Public Safety Specific Testing

In addition to the tests and Key Performance Indicators (KPI's) currently used for operator acceptance in the commercial world, the PSCR will need to verify that the network meets certain minimal criteria that are specific to public safety. Some of the public safety specific test areas noted in section 5 will need to be covered in a comprehensive entrance criteria specifications. The latest version of the PSCR's evaluation network test plan includes some tests that are outside the scope of commercial network testing. The KPI's listed are as follows:

- Outgoing Adjacent Band Interference
- In Coming Adjacent Band Interference
- SNR vs BLER
- SNR vs CQI
- SNR vs Throughput
- Cell Loading
- 2nd Order Harmonic Interference to GPS

Above even what is currently specified there will need to be acceptance criteria based on security and authentication in real world scenarios. Aeroflex further proposes that any network equipment being accepted into the PSCR demonstration network demonstrate performance in the following key areas:

- Policy and Charging Rules Function (PCRF) capacity verification
 - Generate a number simulated UEs on a cell attached to a EPC
 - Perform high no. of transactions which generate PCRF records.
 - Benchmark max no. of simultaneous transactions the policy system can handle

- Benchmark max throughput handling of transactions that interface on OSS/BSS systems
- Security under load
 - Credentialing, Authentication
 - Access classes, QoS
 - Etc

6.2.4 PSCR Evaluation Network

Since the PSCR is not a network operator and cannot limit the infrastructure equipment that is submitted to their evaluation network, they minimally need to impose limits on the quality of infrastructure equipment that is evaluated for public safety. Without these entrance criteria, the PSCR is at risk of becoming a bottleneck in the process of rolling out the public safety network. Additionally, it is inefficient and time-consuming to troubleshoot and resolve issues at the evaluation network. Allowing defects and problems in the infrastructure equipment this late in the process will further delay the rollout of the public safety network.

To further ensure that defects are found early in the process and prevent rollout delays, with help from industry, the PSCR will ideally document a standard test configuration and environment for running test cases in the laboratory. This will include detailing acceptable test equipment, test parameters and preferably automated test suites.

6.2.4.1 Evaluation Network Entrance Criteria

Only once the entrance criteria have been met, infrastructure vendors may submit their equipment to the PSCR evaluation network. Although the PSCR will not publish the individual vendor test results, they will ideally publish the test process and encourage public safety entities to purchase infrastructure equipment only from vendors that have passed the PSCR evaluation network test. If a vendor refuses to show results, the public safety entity should be discouraged from purchasing their equipment.

Emil Olbrich adds that “As new hardware platforms and new features are deployed on the network, we want to be able to test that continually to ensure that public safety has what they need.”[2]

After the PSCR network evaluation, some public safety entities may still want to perform some testing that is unique to their use case. However, this will be quite rare if the PSCR process is implemented as described.

6.2.4.2 Enforcement

Although this paper does not make any recommendation on enforcement of the process, it is clear that without some external motivation it is unlikely that the process will be adhered to consistently across all public safety entities. As Mr. Thomas points out, “Once a vendor is selected, that vendor obviously must certify that he or she will build a network that is consistent with the specification as interoperable. Once it is built in pieces it has to be certified against the test spec.”[4] Therefore the paper assumes that through a separate but related mechanism public safety entities who install network equipment without first going through the process could be subject to some type of punitive action from the appropriate entity. The action may include any combination of withdrawal of funding, abrogation of spectrum rights or some type of fine. This will, of course, be subject to both federal and local legislation.

7 Conclusions

The dream of a high speed, fully interoperable, nationwide public safety network is now being realized. However, only by leveraging the lessons of the commercial network operators and the very powerful PSCR demonstration and evaluation network, can the national public safety network be rolled out by the currently 50,000 public safety entities across the country. This paper strongly encourages the public safety network administrators to publish and follow the process outlined herein to overcome the many obstacles posed by a poorly organized network rollout.

REFERENCES:

Federal Communications Commission (FCC) Public Safety Homeland Security Bureau's Emergency Response Interoperability Center (ERIC) Interoperability Forum: A Discussion on Creating and Implementing the Technical Framework for the Nationwide Interoperable Public Safety Mobile Broadband Network, March 4, 2011, Panel 1: How to ensure nationwide interoperability for public safety broadband utilizing LTE 4G Technology:

[1.] **Dr. Kenneth Budka**—Senior Director, Advanced Mission Critical Communications, Bell Labs, Alcatel-Lucent

[2.] **Emil Olbrich**—Electronics Engineer, National Institute of Standards & Technology (NIST)

Panel 2: Solutions for the deployment of Radio Access Network equipment to achieve nationwide Operability and Interoperability

[3.] **Jeff Anderson**—Wireless Broadband System Architect. Motorola Solutions, Inc.

Panel 4: Where we go from here

[4.] **Edmond J. Thomas**—Technology Policy Advisor, Wiltshire & Grannis

Full video of the event can be found here:

<http://www.youtube.com/watch?v=JRUEjm--SUU>

APPENDIX A: LTE Overview

What is LTE?

The radio frequency modulation scheme, OFDM (orthogonal frequency division multiplex), and multiple antenna, MIMO (multiple-input and multiple-output), technologies are the key enablers for LTE air interface. The OFDM transmission is robust against interference such as multi-path fading and its operating bandwidth is easily scalable. LTE is able to function at 1.4, 3, 5, 10, 15 and 20 MHz bandwidths allowing flexible use of both new and existing frequency bands. Another important attribute of OFDM is that it works well with MIMO transmission, which is a proven technology that achieves higher spectral efficiency and better cell coverage without increasing transmit power or operating bandwidth.

Benefits of LTE

LTE peak data rates are a significant improvement to the narrow band public safety system. Apart from the peak data rates, LTE system includes technologies designed to achieve robust average throughput under complicated radio propagation environments. LTE is optimised for low to medium speeds (0 ~ 15 km/h), but it also ensures high performance for speeds up to 350 km/h. Now 800 km/h speed is being considered to cope with the recent development of the high speed trains. In addition to higher peak data rates and robust average data rates, wide-area coverage is also being targeted. The throughput, efficiency and mobility targets must be met for 5 km cells through to 30 km cells and up to 100 km cells. The capacity, the mobility, the range and the robustness of the LTE air interface makes its very suitable for public safety broadband network.

Public Safety LTE Spectrum

A portion of the upper 700MHz band has been mandated for FDD LTE deployment with 5MHz uplink and 5MHz downlink as shown in Figure 1. The adjacent D-Block spectrum is also being considered for LTE usage. The public safety 700MHz broadband spectrum and the D--- Block are based on clearing of UHF TV stations 60 – 69 (746 – 806 MHz), in addition to the FCC 2nd, 8th & 9th Notice of Proposed Rule Making (NPRM). If the D-Block is granted for public safety, the LTE system can be easily extended to the D-Block without hardware changes making in total 10 MHz for downlink and 10 MHz for uplink. When coupled with MIMO technology, this system in theory can deliver a theoretical peak throughput of 150 Mbps on the downlink and 32.5 Mbps on the uplink with the LTE release-8 standard.

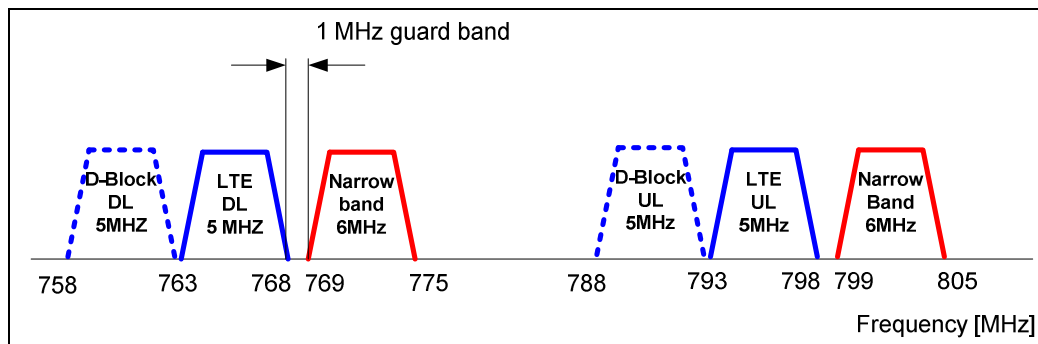


Figure 1: Public safety spectrum allocation over Band XIV.

LTE System Architecture Evolution

Apart from the MIMO/OFDM air interface, the LTE standard also includes the SAE (System Architecture Evolution), which is a flat IP-based network architecture designed to simplify the network to other IP based communications network as shown in Figure-2. SAE uses an eNB and Access Gateway (AGW) and removes the RNC (Radio Network Controller) and SGSN (Serving GPRS Support Node) from the equivalent 3G network architecture. This simplification not only results in a simpler and flatter radio network structure, but also reduces significantly the network latency.

LTE specifies the data packet latency in less than 5 ms in optimal conditions. Note that, in public safety scenarios, the maximal spectrum efficiency may not be essential in situations when minimum latency is required. LTE specifies the C-plane (control plane) latency to be less than 50 ms. This not only improves user experience, but also prolongs the terminal battery life. A fast transition from an idle state to an active state allows terminals to spend more time in the low-power idle state. This in turn means that more users can access the network more quickly. This is highly desirable for the emergency situations in public safety.

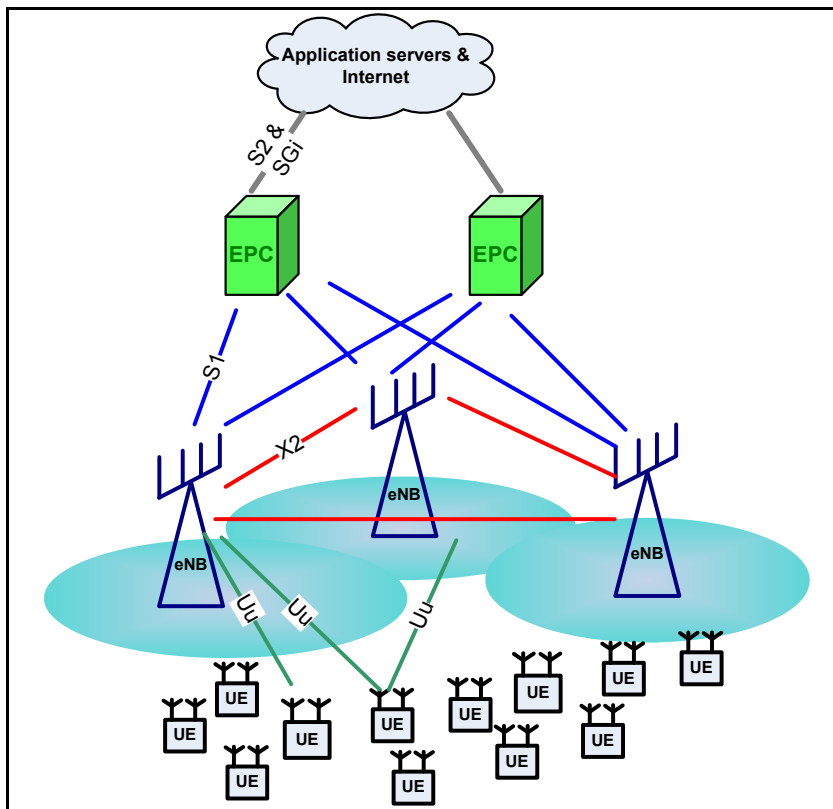


Figure 2: Overview of the LTE SAE.

The simplified network architecture means that, in LTE, many network functionalities have been moved to the eNB, which has to manage radio resource and mobility in the cell and sector to optimize all the UE's (user equipment) communication. Therefore, the performance of LTE depends on heavily on the radio resource management algorithm and the design and implementation of its eNB's. The system developer needs a new approach to evaluate the comprehensive performances of the eNB, which carries out the most complicated functionality in LTE network.

Technology life cycle and integrated test plan

The development of the LTE-based public safety broadband network will be an incremental and iterative process. The process can roughly be divided into five phases. They are the proof of concept phase, the development phase, the conformance phase, the acceptance phase, the deployment phase, the maintenance phase and the improvement & evolution phase as shown in Figure-3.

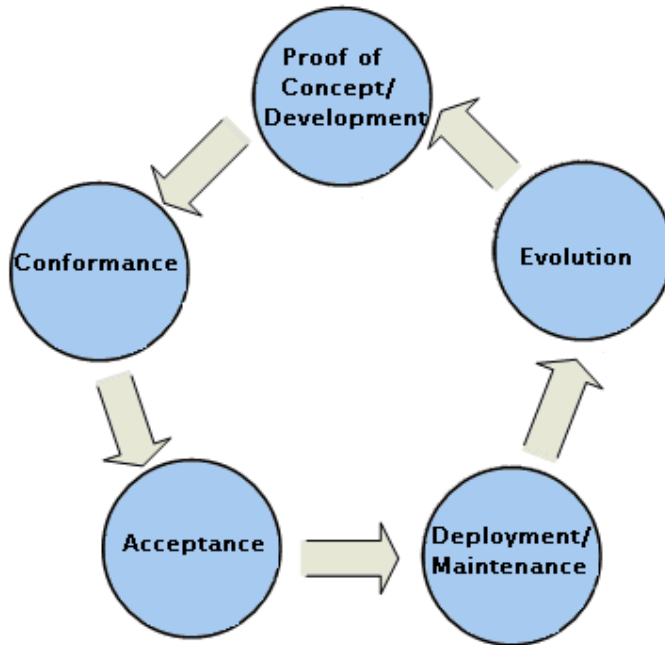


Figure 3: Technology life cycle and integrated test plan.

Proof of Concept and Development

The Proof of Concept phase is to study if the technology is fundamentally feasible for targeted applications. During this phase, the most fundamental aspects such as the RF characteristic, modulation schemes, and their achievable performances in terms of throughput, range, and coverage of the candidate system should be evaluated.

Once it is confirmed that a technology is feasible, the detailed design and development work is carried out. To ensure the correct and in time development of the RF, hardware (HW), firmware, SW and algorithm components, the correct test tools and methods are brought to bear on functional and initial system integration tests.

Conformance

Currently infrastructure vendors must verify that their LTE devices conform to the 3GPP 36.141, the industry conformance specification for LTE base stations. This specification covers almost exclusively RF parametric testing and can be run without connecting to any mobile device, even in emulation. Although this conformance test specification exists under the 3GPP, it is not required by any industry body and is typically enforced on a network operator by network operator basis.

In the public safety space, since there is no single, official network operator, this step must be validated by some other mechanism.

Acceptance

Most commercial network operators have their own specifications and requirements for their selected infrastructure vendors. These are based on the 3GPP specification, but often include proprietary configurations and test environments. This is traditionally performed over the course of lengthy trials where multiple vendors are invited, but only one or two vendors get the operators business. Thus, commercial network operators only have to support a small number of infrastructure vendor's equipment through the deployment phase and beyond.

Again, as public safety has no designated network operator, some other organization must step into perform this acceptance phase.

Deployment/Maintenance

Infrastructure Equipment from many different vendors are used in a practical system during deployment. It is important to ensure this equipment is interoperable. After the equipment has passed the set of conformance and acceptance tests specified in the standard some specially designed interoperability tests (IOT) have to be carried out. The IOT tests are typically performed by the vendors or the network operators using some widely used and highly proven test equipments that are regarded as the *De Facto* industry standard.

After the network is deployed, it is inevitable that the SW and firmware (and HW occasionally) will need to be updated for enhancements or bug fixes. It is important to evaluate the performance and stability of the SW before it is distributed to the real and operating network.

Evolution

LTE is an evolving technology. New features and enhancements are constantly being added by 3GPP to LTE. For example, the positioning and beam forming technologies have now been specified in LTE standard and they will be very useful for improving the performance and usability of LTE-based public safety broadband network.

Before new technologies are deployed, their performance and impact must be evaluated according to the public safety orientated criteria. For example, the investigation might find that the LTE positioning accuracy is inadequate for public safety agencies operate. Moreover the investigation results could be fed back to 3GPP who could potentially tailor their specification to improve the performance. All changes to the specification require iterating back through the conformance and acceptance phases.

As the public safety network evolves and requirements are fed back from the field, the technology and infrastructure must also evolve. Without a healthy and robust test and acceptance process, changes will be onerous to implement and the network will stagnate.

Appendix B: Technology Life Cycle Test Equipment

Proof of concept and Prototyping:

The development and deployment of the LTE-based public safety broadband network is still in the early stage. Although LTE technology looks promising, there are still many technical unknowns for public safety applications. These unknowns and potential problems have to be understood and ruled out before the large investment is made to the large scale development and deployment of the LTE-based public safety broadband network. Some feasibility studies and concept proving prototyping exercises have to be carried out to identify potential problems. During this phase, the fundamental aspects such as the RF characteristic and the achievable physical layer performances in terms of throughput, range, and coverage of the candidate system should be evaluated under the public safety specific conditions.

The 700 MHz frequency band is very good for mobile communications because of its long range and penetration capabilities. It is important to understand the LTE system's performance and behaviour when it is deployed to the 700MHz band, which is not part of the commercial LTE specifications. The LTE-based public broad band network must co-exist with narrow band systems such as P25, LMR and TETRA as shown in Figure 1. But the current LTE specifications and the corresponding acceptance and conformance tests are designed and optimised for the commercial broadband network operations. The RF and physical layer specifications such as maximum transmit power, ACLR, blocking scenario, and fixed-reference channels will have to be adjusted for the 700MHz band and for the existing narrow band public safety system. The LTE transmitter must operate without giving interference to the adjacent narrow band system that is only 1 MHz away and the LTE receiver must be able to operate in the presence of a high powered 12 kHz signal from the narrow band system which was designed previously without considering the LTE deployment. The LTE transmitter for both eNB and UE might have to limit its maximum transmit power and refine its spectral mask. On the other hand, the LTE receiver for both eNB and UE might have to improve its channel selectivity and increase its dynamic range and sensitivity. These changes will have impacts on the achievable throughputs on uplink and downlink and will need to be evaluated carefully to understand what the expected performance should be.

The achievable performance of a practical system is not only limited by the core transmission techniques, but also affected by all supporting physical layer procedures such as random access channel, paging channel, power control, control channel, broadcast channel, handover measurements, feedback information calculation, and synchronization procedure. These procedures can become the dominant system performance limiting factor if they are not designed and tested properly and a lot of the development and debugging efforts are spent in making sure these procedures working correctly and robustly for the commercial LTE system. The operational parameters and configurations of these procedures could change for the public safety deployment. But the system designer needs to be able to measure the behaviour and performance of these procedures before making changes to their configurations and parameters.

The concept proving study is typically carried out by of some theoretical link budget calculations and computer simulations. These analytical results should then be used as guidance for implementing the core technologies on the real-time target prototyping platform, which can be used in the lab and in the field as shown in Figure-2.

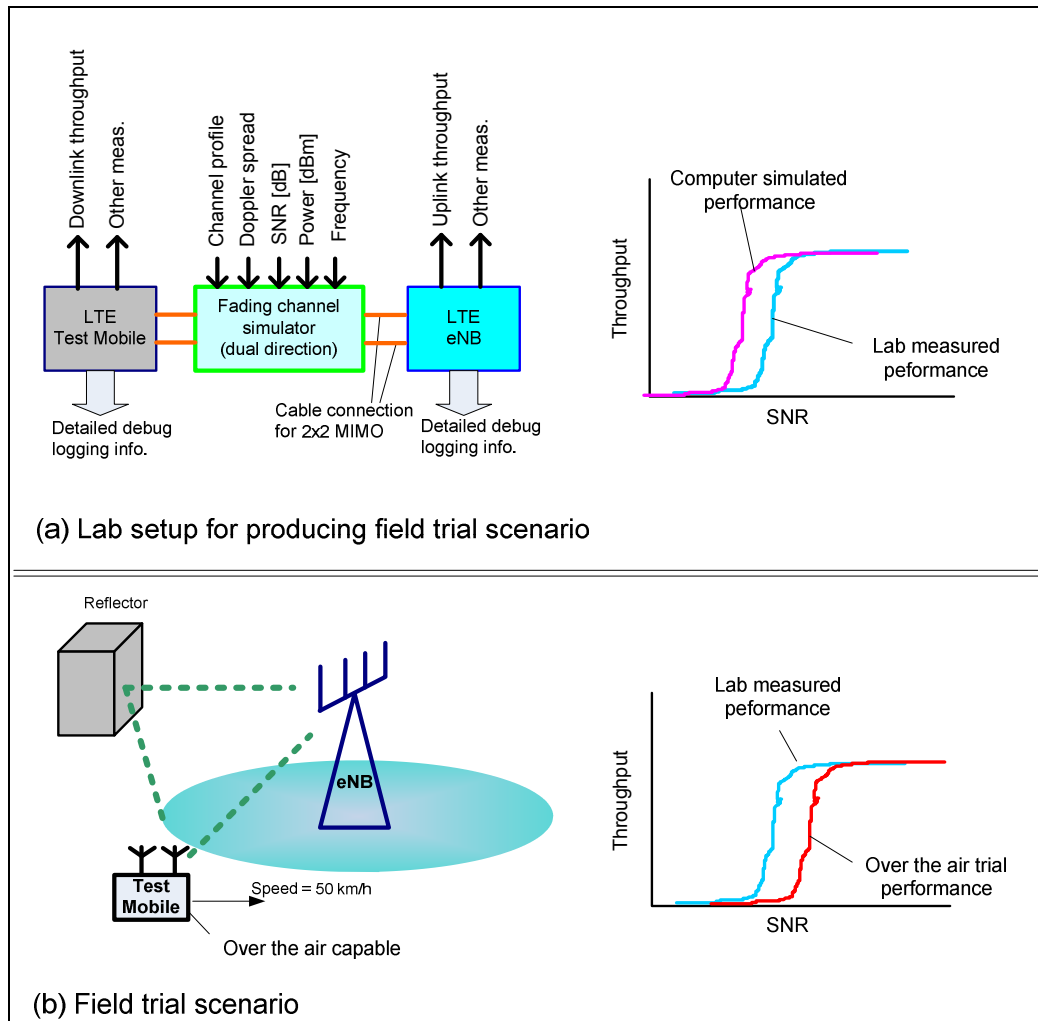


Figure 2: Concept proving trial and its lab setup.

The prototyping platform should be a very flexible, powerful and high performance SDR (software defined radio) platform consisting powerful DSP/FPGA cards and high performance RF front-ends. The researcher and the system developer can develop fully or partly the candidate system on these platforms. For example, the researcher can try the beam-forming scheme for the public safety network before it is even commercially deployed. At this stage, the system/algorithm specifications are new to the system developer. They will be interested in validating their theoretical analysis and simulation results by implementing their systems and algorithms on the real-time equipment and over practical RF propagation channels.

If the field trial results do not match the theoretical results, the system developer will then be able to analyse the logging information to identify the root causes and purposed solutions. However, doing fully scale field trials over the air might not always be feasible. For example, the required frequency band might not be available because of the regulation. The system developer can still emulate the OTA trial using fading channel simulator in the lab. The fading channel simulation setup with the prototyping platform makes it easy for the system developer to create OTA channel conditions in the lab in a very controlled manner and to compare easily the simulated results to the measured results to identify and minimise the implementation loss.

The concept proving phase is essential for development and deployment of any new systems. It confirms the technological feasibilities, accumulates know-how's and generates guidelines for the further development works. The key to the concept proving phase is to develop a flexible and powerful prototyping test platform that allows the system developer to experiment with the new technologies early on, so that they can close the gap between theoretical analysis and practical development.

Development and functional test platform:

Once it is confirmed that a technology is feasible, the detailed design and development works are to be carried out. To ensure the correct and in time development of the RF, HW, firmware, SW and algorithm components, the correct test tools and methods have to be made available to conduct a large amount of the functional tests and initial system integration tests. The development test solution must give detailed debugging information and enable test case creation over vary large parameter space including the special corner cases.

To develop the full protocol stack LTE eNB and UE is a huge task. It is typically divided into different protocol layers and is carried out by different teams. The higher layer protocol will typically not be available and engineers must configure the physical and lower layer tests using scripts that may incorporate hundreds of LTE parameters. The development test solution must enable incremental testing at Layer 1, Layer 2 or higher layer levels, and together with a graphical user interface, engineers can configure parameters and scripts to execute complex tests scenarios at different layers. The concept of the incremental eNB test solution is shown in Figure-3.

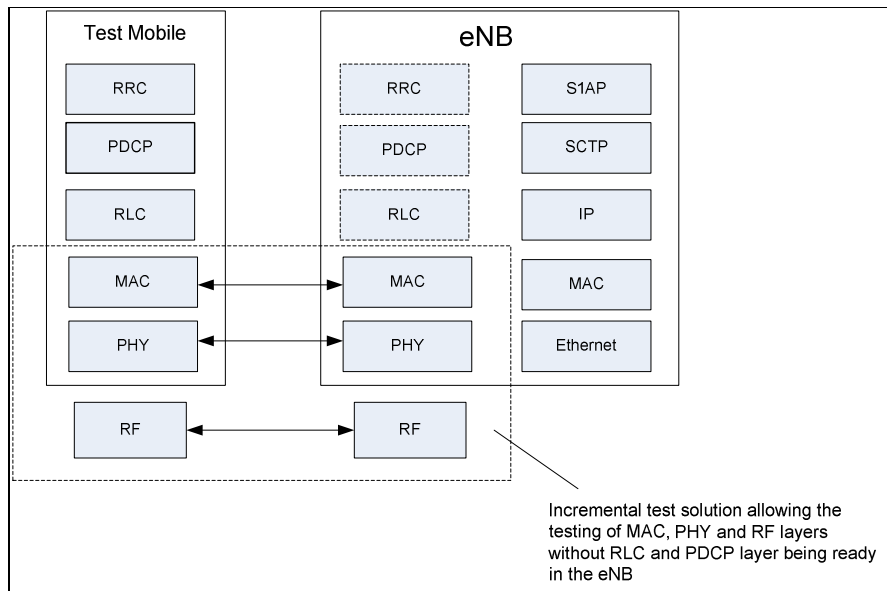


Figure 3: Incremental development test solution.

In order to achieve the extensive test coverage over the huge parameter space over the different LTE protocol layer, the development test solution should also support full local or remote automation of test scripts, which is essential when building extensive and repeatable testing. The test script configuration tool enables the generation and management of scripts that can then be initiated manually or by an executive test entity. The development test solution should also make it possible to alter parameters in real time to extend test coverage across a wide range of different configurations used in a live system. This enables early detection of software bugs that may not otherwise be found until much later in the development cycle when diagnosing and rectifying errors is typically much more expensive.

In LTE, the eNB is the most complicated network element and the scheduler is the most complicated component in the eNB. The scheduler manages (potentially every 1 ms) the resource allocations (time and frequency) to the UE's in the cell according to the channel quality information (CQI) reported by these UE's. Based on the reported CQI and the QoS requirements, the scheduler computes the optimal resources allocation scheme that serves all UE's fairly and efficiently. The scheduler algorithm is not specified by the LTE standard and it is a major performance distinguisher for the eNB's from different vendors. The scheduler design might change to incorporate the new efficiency and priority requirements for public safety applications.

It is difficult to test or to optimise the scheduler using field tests that are very difficult to replicate. The common approach used in commercial LTE development is to use an emulated multi-UE system as shown in Figure-4. This test setup allows the developer to control precisely the mobility profile for each UE in the system, so that they can create specific scenarios that cause problem for the eNB scheduler. Then they can adjust the scheduler parameter or algorithm and rerun the test until it gives good enough results. The key to this test solution is that the developer has full and precise control of the emulated mobility scenario. For example, the number UE's can be set to 2 and then to 100 suddenly.

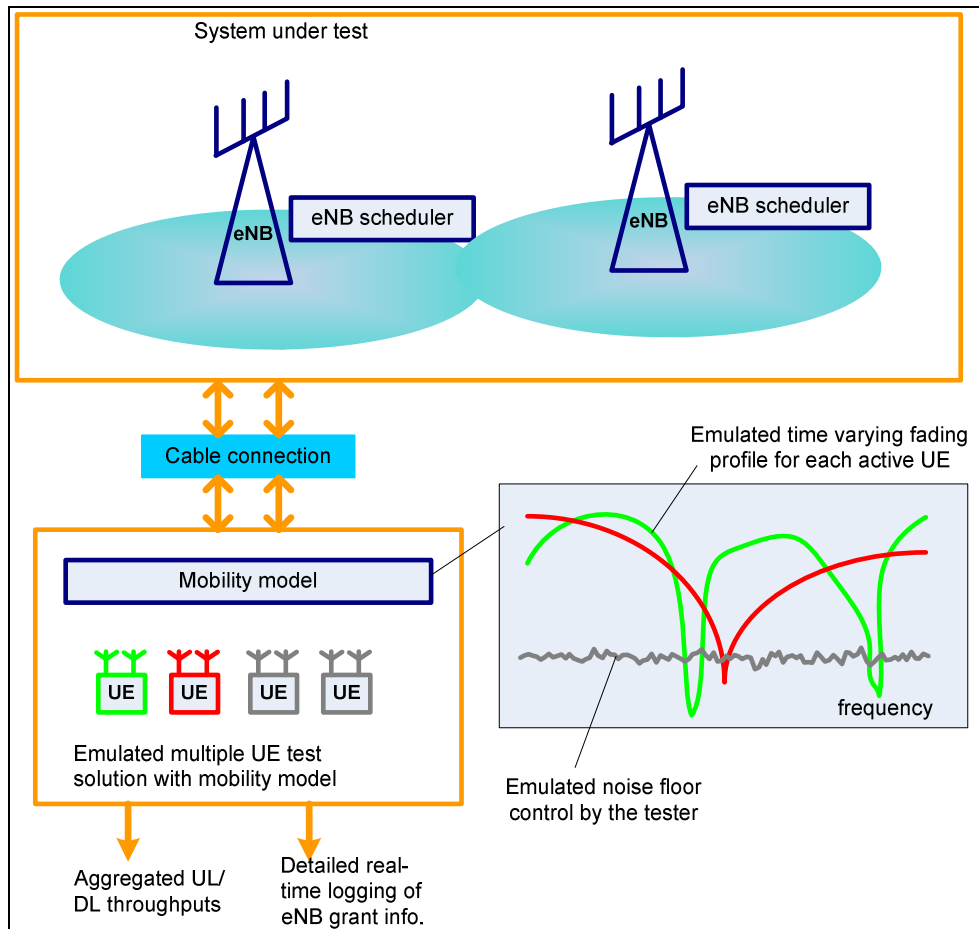


Figure 4: eNB scheduler test solution.

End-to-end and system test platform:

The end-to-end test solution is an extension of the emulated multi-UE test platform and it is required in order to include more network elements and test across all protocol layers. The top-level illustration of the end-to-end test solution is given in Figure-5. The test solution is used in the infrastructure integration phase after the network elements have been developed and tested. This test system emulates a few thousand UE's. Each UE has its own mobility, traffic and application models. The system developer can emulate very realistic and large scale network scenarios including the eNB and the core network elements. This test solution evaluates the capacity of the overall network by generating a lot of loadings from the UE's helping to identify the bottleneck. For example, the system developer might find that the system capacity is limited by the backhauling from the eNB to the core network under certain traffic conditions.

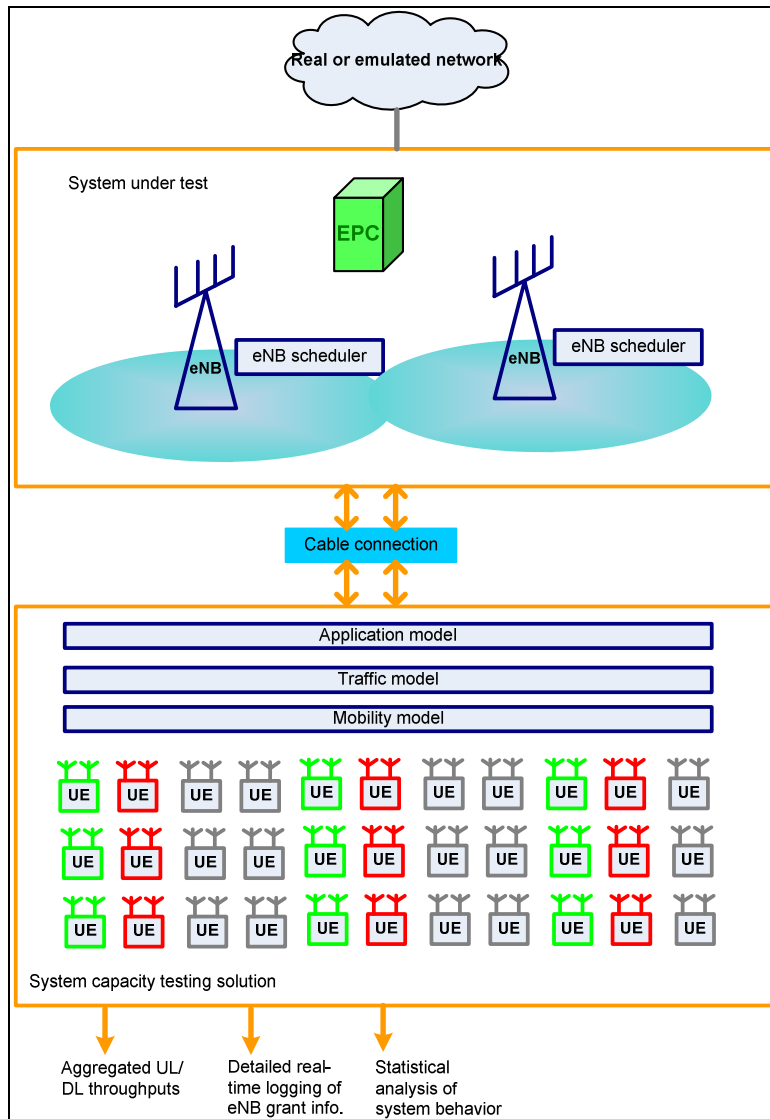


Figure 5: System capacity test solution.

The end-to-end test solution will also be very useful during the deployment and maintenance phases. It is likely that equipments (base stations and UE's) from many different vendors are used in a practical system during deployment. It is important to ensure these equipments are compatible. All equipments must pass the set of conformance and acceptance tests specified in the standard. The conformance tests are necessary but not sufficient. Some specially designed and larger scale interoperable test (IOT) tests have to be carried out. The IOT tests are typically done by the vendors or the operators using some widely used and highly proven test equipment that are regarded as the *De Facto* industry standard.

After the network is deployed, it is inevitable that the SW and firmware (and HW occasionally) will need to be updated for enhancements or bug fixes. It is important to evaluate the performance and stability of the SW before it is distributed to the real and operating network. If the new SW crashes after it is released, it will take time to have it fixed and it might cause network outage. This is especially important for public safety network that has to be operational 24x7x365. Therefore, the SW changes must be tested and evaluated extensively in a lab test environment that emulates the real and operational networks. The commercial LTE vendors normally test their new SW or system releases using a set of very comprehensive tests non-stop for at least 2 weeks before the new SW is released to the field. This testing requirement should be much stricter for the public safety broadband networks. For example, the emergence preparedness test scenarios that are specific to public safety should be run for every SW change and system upgrade. The end-to-end test solution is effectively acting as the regression test system for the continuing upgrade and maintenance work for the deployed network.

Development and testing flow chart:

The development and deployment of the LTE-based public safety broadband network infrastructure is a very complicated engineering process. The system developer must put in place the effective test solutions at different stage of the technology development as shown in Figure-6 below

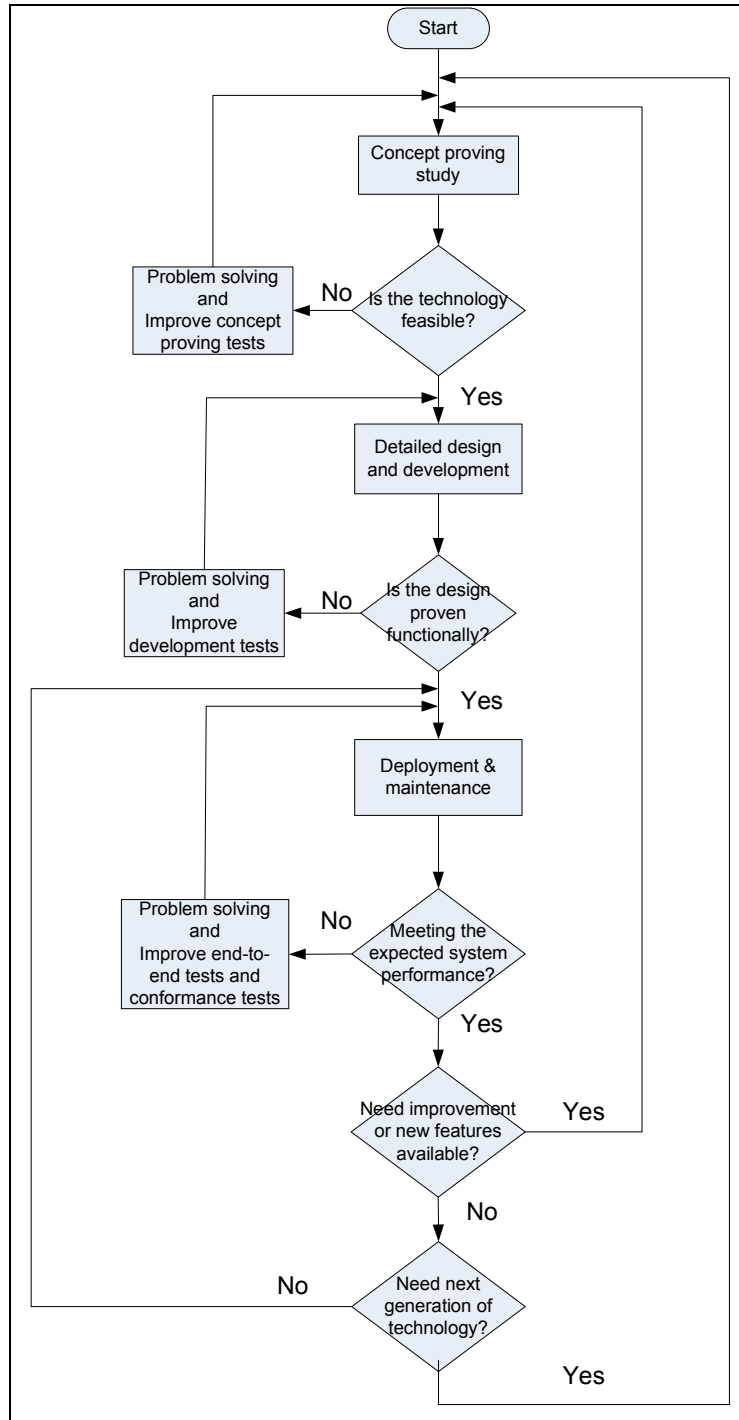


Figure 6: Development and testing flow chart.

Appendix C: KPI Complete List

1. RF transmit accuracy

The LTE public safety system must not interfere with the current public safety system, which is mission critical. The guard band is only 1 MHz wide between the allocated LTE band and the current band. Therefore, the new LTE equipments must be tested for their RF transmit accuracies including carrier frequency, power and spectrum emission mask. These tests have to meet the public safety RF performance requirements that could be more demanding than the commercial LTE requirements.

2. RF receive selectivity

The LTE public safety system has to co-exist with the current narrow band public safety system, which was designed without considering the LTE deployment in its adjacent channel. Its adjacent channel leakage could interfere with the LTE system. The LTE equipments (both UE and eNB) shall be evaluated in the presence of the operating narrow band system to ensure the expected LTE benefits is achievable.

3. Building penetration

The public safety system requires 100% coverage. The 700 MHz is known for its good coverage and penetration capabilities. However, the commercial LTE standards and equipments are designed and optimised for commercial radio frequencies and propagation conditions. The LTE equipments shall be re-evaluated and tested using the public safety spectrums in certain public safety specific propagation scenarios, for example, indoor, in tunnel, underground and remote rural areas.

4. User experience: voice and data quality

The public safety systems convey real-time and mission critical information, therefore, it is important that the LTE system delivers clear voice and data communication qualities that meet the public safety requirements.

5. Aggregated throughput and UE fairness

The eNB throughputs heavily depend on the MAC (media access control) layer scheduler designs on both the uplink and the downlink. The different eNB vendor could design and optimise their schedulers according to different criteria, such as traffic conditions, re-transmission buffer occupancies, response time etc. The most important metrics for indicating the eNB scheduler performance are:

- The aggregated eNB throughputs on both downlink and uplink including all UEs
- And the UE fairness, i.e. the average throughput achievable for each UE

6. Maximum number of registered/idle UEs

The 3GPP LTE standard does not specify the maximum number of UEs that are registered to the eNB or the network. The LTE equipment vendors might design their eNB/network to support different maximum numbers. There needs to be a test plan and a test solution to validate and ensure the different equipment from different vendors meeting the public safety application requirements.

7. Maximum number of active UEs

The maximum number of active UEs that are being addressed by the eNB in the connected state are not clearly specified in 3GPP LTE standard. Different vendors might have different design target and capacity. Therefore test plan and test solution have to be in place to ensure the consistence of the LTE equipments for public safety deployment.

8. RACH and Paging capacities

The eNB's RACH and paging capacities are one of the important aspects of the system accessibility, which is most important for public safety applications. We need test solution that is able to generate > 10,000 RACH and paging procedures within seconds to stress test the LTE public safety system.

9. Tracking area update accuracy

The UE location update provides valuable info. The accuracy of the UEs mobility update needs to be evaluated, especially for large number of multiple UE scenarios.

10. Stability and robustness

The system stability includes SW, HW and FW stabilities. The public safety network is required to be operational 24 x 7 x 365. We must develop stress test solution to evaluate stability and robustness before any system is deployed and before any SW, HW and FW upgrades are applied to the already deployed networks.

11. Power efficiency

The public safety system needs to be operational on battery power after the main power sources are cut off due to a natural disaster for example. It would be beneficial to deploy the power efficient LTE equipment for public safety systems. We need test solution to evaluate the power overall power consumption of the LTE equipment under different traffic loading conditions.

12. Basic interoperability

It is likely that a LTE public safety network consists of network equipment for multiple vendors. The basic interoperability must be evaluated in the lab before deployment. The basic interoperability tests should not only evaluate the different network entities (UE, eNB, MME, S-GW, P-GW, PCRF etc), but also the physical and logical interference between these entities (uu, S1-MME, S1-U, S11, S6a, X2 etc).

13. MME interoperability and pooling efficiency

Every LTE eNB could connect to multiple MME entities. The loading of these MMEs needs to be balanced efficiently, such that the network entities are evenly utilised and there will be no large latency in handling the services. It is important to check that the MMEs from different vendors are interoperable.

14. S-GW interoperability and selection efficiency

Each MME could communicate to multiple S-GW depending of the network topologic and traffic types. We have to ensure the S-GW select is done correctly and efficiently. This is done by emulating a large amount of active UEs with different traffic types. This is also an important interoperability test for the S-GW from different vendors.

15. Robustness of broadcast info

Broadcast messaging could be an important feature in mission critical operations. If some broadcast transmissions means (such as eMBMS) will be used, it is important to verify the robustness of the broadcasted messages.

16. Jamming rejection capabilities

Public Safety Network should work in every condition and it is important to verify the robustness of the Public Safety network to possible electronic attacks in form of jamming.

17. Redundancy

Public Safety network should work in extreme scenarios. If some of the nodes go down for whichever reason (attack, fire, meteorological event, etc ...) the network should be able to keep working. Presumably, network planning will then allow for some redundancy that will have to be tested. In particular it should be tested that shutting down some of the nodes, the network could still be working with the desired coverage and capacity.

Appendix D KPIs Table

The following table collects and summarizes the top-level network infrastructure KPIs (key performance indicator) for the different areas and the different stages of an LTE network deployment.

	User plane	Control plane	Management plane	Security plane	Interoperability
Pre-deployment	<ul style="list-style-type: none"> • Peak DL/UL throughputs • Link adaptations • UL/DL schedulers • Avg. throughputs under fading • eNB transmit EVM • eNB transmit spectrum • User plane round trip time • Packet jittering • LTE diversity options • Call setup time • Robustness of broadcast info (such as eMBMS services if used) 	<ul style="list-style-type: none"> • Paging channel detection probability • RACH detection probability • Overloading RACH request • Call dropping probability • Control plane round trip time • Cell search performance • End to end latency • Maximum number of supported users with a minimum guaranteed service) 	<ul style="list-style-type: none"> • Load balance between eNBs • QoS characterization • EPC mobility management • Jamming rejection capabilities • Power consumption • Stress test • Reboot time • Device blocking capabilities 	<ul style="list-style-type: none"> • Pre-emption • Authentication 	<ul style="list-style-type: none"> • 3GPP internetworking
Field trials	<ul style="list-style-type: none"> • Achievable throughput in the field • Cell edge throughput • Initial coverage and range • Indoor and outdoor • Link budget validation 	<ul style="list-style-type: none"> • Handover success probability • Handover time • Handover performance 			
Deployment	<ul style="list-style-type: none"> • Drive tests • Capacity & traffic density • Antenna properties 	<ul style="list-style-type: none"> • Cell interference mitigation • 	<ul style="list-style-type: none"> • X2 interface capacity • Redundancy (UEs still working when a eNB goes down) 		
Post-deployment	<ul style="list-style-type: none"> • Software stability tests for updates • Network parameters optimization 	<ul style="list-style-type: none"> • Network parameters optimization 			